Before the Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Rules and Regulations Implementing the Truth in Caller ID Act of 2009	)	WC Docket No. 11-39
	)	

Comments of the Privacy Rights Clearinghouse

The Privacy Rights Clearinghouse (PRC) respectfully submits the following comments to the Federal Communications Commission (Commission) for its consideration with respect to its call for public comment in its Notice of Proposed Rulemaking in the Matter of Rules and Regulations Implementing the Truth in Caller ID Act of 2009, WC Docket No. 11-39.

I. Background

The PRC is a nonprofit organization, established in 1992 and located in San Diego, California.[1] Our mission is two-part: consumer education and consumer advocacy. We have published more than 50 Fact Sheets that provide practical information consumers may employ to safeguard their personal information, and we invite individuals to contact the organization with their privacy-related questions, concerns and complaints.

II. General Statements

Caller ID spoofing services allow users to manipulate caller identification information so that when transmitted a receiving party will believe the call is originating from someone or someplace else. These services are widely available, and unfortunately they are largely used to harm and commit crimes against consumers.

[1] Privacy Rights Clearinghouse, www.privacyrights.org (last visited Apr. 22, 2011).

As a consumer privacy organization, Privacy Rights Clearinghouse has an interest in advocating against the use of caller ID spoofing services to defraud consumers, rob them of control over personal data, and/or put an individual's physical safety at risk. However, we must also support the legitimate uses of caller ID spoofing services that aid in protecting consumer privacy and anonymity when used without ill intent. The rules implementing the Truth in Caller ID Act of 2009 (the Act)[2] must be drafted clearly and sufficiently deter malevolent caller ID spoofing, but they must also allow for legitimate uses.

As the Commission makes clear in its Notice of Proposed Rulemaking (NPRM),[3] caller ID spoofing has been used increasingly as a means to trick consumers into providing information that may be used to defraud or commit identity theft. Stalkers and harassers may use spoofing services to call individuals who seek to avoid contact with the spoofer but are tricked into answering due to misleading caller ID information displayed by the called party's caller ID service.

Criminals may also use spoofing services in a manner that risks causing injury to innocent individuals in the form of "swatting," or manipulating caller ID information to direct armed law enforcement SWAT teams' response to bogus situations.[4]

Despite its potential to cause harm, caller ID spoofing may also be used for legitimate purposes that the Act is intended to permit.[5] For example, domestic violence victims may need

---

[2] Truth in Caller ID Act of 2009, Pub. L. No. 1111-331, codified at 47 U.S.C. § 227(e).

[3] FCC, In the Matter of Rules and Regulations Implementing the Truth in Caller ID Act of 2009, Notice of Proposed Rulemaking, Rel. Mar. 9, 2011, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-11-41A1.doc [hereinafter NPRM] .

[4] *See e.g.* Henry K. Lee, *Illinois man accused of fooling S.F. cops*, S.F. CHRONICLE, March 11, 2011, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/03/10/BA6L1I88UN.DTL (an Illinois man allegedly used a caller ID spoofing service to trick San Francisco police into responding to bogus incidents).

to transmit caller ID information to complete a call to a phone set up to block private numbers, but risks her safety if she reveals her true location. Also, some professionals (such as a doctor) may want an office number to show up in caller ID information rather than a cell phone number that they wish to keep private. Therefore, the implementing rules must refrain from discouraging valid uses through vague language.

Caller ID spoofing services provide a dangerous tool in the wrong hands, but are invaluable to those who use them without ill intent. We encourage the Commission to implement the Act in a manner that sufficiently deters and punishes bad actors, yet clearly permits legitimate uses.

III. Responses to Specific Inquiries

A. Proposed Amendments to the Commission's Rules Relating to Calling Party Numbers

Para. #13: The Commission seeks comment on the use of the word 'knowingly' in the statute and proposed rules.

The Commission's proposal to change the placement of the word "knowingly" in the rules from its placement in the statutory language affects the rules' interpretation in a concerning manner. In the proposed rules, the word "knowingly" refers to the required state of mind of the person/entity causing the caller ID service to transmit or display misleading or inaccurate caller ID information.[6] In contrast, "knowingly" in the Act's language appears to refer to the state of mind of the caller identification service in displaying or transmitting the information.[7]

---

[5] *See Truth in Caller ID Act, Report of the Committee on Commerce, Science, and Transportation*, S.30, 111-96 (2009).

[6] "No person or entity in the United States, shall, with the intent to defraud, cause harm, or wrongfully obtain anything of value, **knowingly cause**, directly or indirectly, any caller identification service to transmit or display misleading or inaccurate caller identification information." C.F.R. § 64.1604(a) (2010) (emphasis added).

[7] "It shall be unlawful for any person within the United States in connection with any telecommunications service or IP-enabled voice service, to cause any telecommunications service or IP-enabled voice service, to cause any caller

In its NPRM, the Commission explains the change by stating, "in many instances, the caller identification service has no way of knowing whether or not the caller identification information it receives has been manipulated."[8] While this may be accurate, it does not explain why under the Commission's proposed rules, the party with the requisite ill intent may also now need to knowingly cause the transmission or display of misleading or inaccurate information to violate the Act. The Act's prohibition already states that the person or entity must have the "intent to defraud, cause harm, or wrongfully obtain anything of value." Therefore, the requirement that the bad actor also act "knowingly" to cause transmittal or display of misleading/inaccurate caller ID information may add an unnecessary hurdle to successful enforcement by having to show both knowledge and intent.

We urge the Commission to modify the rule so that spoofing services are prohibited from knowingly transmitting misleading or inaccurate information for a party violating the act, or retain the language in the Act's rather than replace it with the language in the proposed rulemaking. We believe that under either circumstance the Act's purpose of preventing fraudulent or intentionally harmful spoofing will be better served than it is under the proposed rules.

Para. #14: The Commission seeks comment on whether the proposed prohibition on causing any caller ID service to transmit or display "misleading or inaccurate" caller ID information with the "intent to defraud, cause harm, or wrongfully obtain anything of value" provides the public with "ascertainable certainty" about what would constitute a violation of the Act?

Adopting specific definitions of words such as "defraud" and "harm" may pose the danger of creating loopholes for those using spoofing for nefarious purposes. Therefore, we

---

identification service to **knowingly transmit** misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value." 47 U.S.C. § 227 (e)(1) (2009) (emphasis added).

[8] *See* NPRM, *supra* note 2, at 7.

advise the Commission to refrain from defining such terms, especially in a narrow manner. Nonetheless, the public must be educated on the meanings of the words "defraud" and "harm" in the context of the Truth in Caller ID Act of 2009. For example, we believe it would be helpful for consumers if the Commission's Consumer and Governmental Affairs Bureau published a guide on the Truth in Caller ID Act on its website and/or updated its existing publication titled "Caller ID and Spoofing."[9] This would help to ensure that those who seek to use spoofing for legitimate purposes are not discouraged from doing so. Without additional guidance and informational materials, individuals may believe that "defraud" is synonymous with "deceive," in which case those engaging in legitimate spoofing may refrain to make sure they are not in violation. Caller ID spoofing is arguably always used for deceptive purposes, so it is important that the rules be drafted so they do not chill legitimate uses.

Para. #21: Third-Party Spoofing Services

The Commission seeks comment on whether it should adopt rules imposing obligations on providers of caller ID spoofing services, and what rules it can adopt to discourage or prevent caller ID spoofing services from enabling or facilitating unlawful conduct?

As the Commission notes, caller ID spoofing services facilitate both lawful and unlawful caller ID manipulation. In its January 2011 letter to the Commission, the Department of Justice (DOJ) has urged the Commission to "consider the feasibility of requiring public providers of caller ID spoofing services to make a good-faith effort to verify that a user has the authority to use the substituted number, such as by placing a one-time verification call to that number."[10]

---

[9] Federal Communications Commission, Caller ID and Spoofing, FCC Consumer Facts, http://www.fcc.gov/cgb/consumerfacts/callerid.html (last visited May 2, 2011).

[10] *In the Matter of Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, WC Docket No. 11-39, Letter from Lanny Breuer, Assistant Attorney General, Dep't of Justice, to Marlene Dortch, FCC, at 4 (Jan. 26, 2011).

The PRC believes it would be appropriate to impose rules on caller ID spoofing services, and urges the Commission to consider doing so. Otherwise, the Commission risks implementing the Act in a way that does little to reduce harms caused by the misuse of spoofing services. Spoofing services should at minimum be prohibited from both inducing malevolent spoofing (through its marketing materials)[11] and knowingly transmitting misleading caller identification information intended to defraud, cause harm or wrongfully obtain anything of value. For example, it may be appropriate to require that any user of a spoofing service assent by phone or click-through agreement (in the case of online calls), prior to making the call or signing into the spoofing service, that they are not using the service for illegal purposes. Another possibility is to require spoofing services to institute a complaint process and terminate access to the service for users who have had a certain number of complaints filed against them. At minimum, spoofing services should be required to post prominent disclosures in visual and/or audio form that draws their customers' attention to the Act. As mentioned above, the DOJ has also proposed requiring services to place verification calls. We urge the Commission to consider the feasibility of regulating spoofing services or holding them vicariously liable in situations where they clearly facilitate forms of spoofing that the Act seeks to prohibit.

[11] For example, in the FAQ section of its website, SpoofCard lists the question "Is SpoofCard Legal?" The answer below does not mention the Truth in Caller ID Act, and is very vague , stating "Each of the capabilities of SpoofCard is legal in the US. However, certain uses may be illegal depending on which state you are calling from or to. For example, a handful of states have passed laws that make it illegal to spoof caller ID for certain purposes, such as 'to mislead, defraud, or deceive the recipient of a telephone call. Before using the spoofing capability of SpoofCard, you should determine whether the use you will make of the service is legal in the state where you are calling from and the state where the party you are calling is located." SpoofCard, http://www.spoofcard.com/faq (last visited Apr. 22, 2011).

Para. #23: Need for Additional Exemptions

The proposed rules exempt from its regulations any authorized law enforcement activity and court orders specifically authorizing caller ID manipulation.[12] We do not specifically advocate adding an exemption, but urge the Commission to consider the possibility of doing so to protect victims who engage in legitimate uses of spoofing to maintain personal privacy and safety. For a viable proposal detailing adding an additional exemption to cover Victim Service Providers,[13] we refer the Commission to the comments in this proceeding submitted by the National Network to End Domestic Violence. [14]

Regardless of the means by which it is accomplished, the proposed rules implementing the Truth in Caller ID Act must not chill legitimate uses of caller ID spoofing.[15]

Para. #27: Services offering the ability to unmask a blocked number

The Commission seeks comment on whether it is appropriate to impose obligations on carriers and VoIP providers to prevent third parties from overriding calling parties' privacy choice?

Blocking a calling number is explicitly permitted under the Act. Some services offer the ability to unmask a blocked number by stripping privacy indicators chosen by the calling party.[16] Because call blocking is explicitly permitted and consumers may rely on its effectiveness in seeking to protect their privacy, we believe that calling party choice should be honored with respect to caller ID blocking.

---

[12] *See* C.F.R. § 64.1604(b)(1)-(2).

[13] National Network to End Domestic Violence uses the definition found in the Violence Against Women Act of 1994. 42 U.S.C. § 13925(a)(36)(2010).

[14] *See* Comments of National Network to End Domestic Violence, In the matter of Rules and Regulations Implementing the Truth in Caller ID Act of 2009, WC Docket No. 11-39, submitted Apr. 18, 2011, at 6.

[15] *See*. S. Rep. No. 111-96, at 2 (2009) (the Commerce Committee Report recognizes the legitimate uses of spoofing, especially those pertaining to domestic violence).

[16] *See* NPRM *supra* note 3 , at footnote 49 (The footnote mentions www.trapcall.com which is owned by TelTech, the company that also owns a spoofing service called SpoofCard).

IV. Conclusion

As the Commission implements the Truth in Caller ID Act of 2009, we urge it to balance the need to protect consumers from harmful spoofing with the place for legitimate uses of spoofing. In doing so, the PRC believes that the Commission should reconsider its change in placement of the word "knowingly" in its proposed rules, provide consumers with resources to inform them of the scope of the Truth in Caller ID Act of 2009, and consider imposing rules on spoofing services so that they are at minimum required to run their businesses in a manner that is not contrary to the Act's purpose of reducing malevolent caller ID spoofing.

Respectfully Submitted,

Beth Givens, Director
Meghan Bohn, Staff Attorney
Privacy Rights Clearinghouse
3100 5th Ave. Ste. B
San Diego, CA 92103
www.privacyrights.org